Leçon 122 : Anneaux principaux et applications

I - Notions de PGCD et PPCM dans un anneau principal

I-A. Anneaux Principaux

déf ① : On dit que A est un anneau principal si : A est intègre et tout idéal I de A est principal, i.e engendré par un seul élément.

exemple ② : $\mathbb{Z}$ et $K[X]$ (avec K un corps)

I-B. PGCD et PPCM

déf ③ : Si $(d,a,b) \in A^3$ alors d est un PGCD de a et b si $(d) = (a,b)$

déf ④ : Si $(d,a,b) \in A^3$ alors m est un PPCM de a et b si $(m) = (a) \cap (b)$

remarque ⑤ : ces définitions coincident avec celles sur un anneau A non principal :

* d PGCD de a et b si $d|a$, $d|b$ et $\forall d' \in A$, $[d'|a \text{ et } d'|b] \Rightarrow d'|d$
* m PPCM de a et b si $a|m$, $b|m$ et $\forall m' \in A$, $[a|m' \text{ et } b|m'] \Rightarrow m|m'$

remarque ⑥ : un PGCD n'est pas unique. Si d et d' deux PGCD de a et b alors il existe $c \in A^\times$ tel que $d = cd'$ (idem pour un PPCM de a et b)

proposition ⑦ : d est PGCD de a et b ssi $d|a$, $d|b$ et il existe $(u,v) \in A^2$ tel que $d = au + bv$

remarque ⑧ : on restreint l'étude au PGCD car si d et m sont PGCD et PPCM de a et b alors il existe $c \in A^\times$ tel que $cdm = ab$

I-C. Construction d'un PGCD dans un anneau euclidien

définition ⑨ : On dit que A est euclidien si A est intègre et il existe $\varphi : A\setminus\{0\} \to \mathbb{N}$ tel que $\forall (a,b) \in A \times A\setminus\{0\}, \exists q,r \in A^2$, $\begin{cases} a = bq + r \\ \varphi(r) < \varphi(b) \end{cases}$

exemple ⑩ : $\mathbb{Z}$ et $K[X]$ sont euclidiens avec $\varphi = \deg$ sur $K[X]$

proposition ⑪ : Si A est euclidien alors A est principal

théorème ⑫ : (algorithme d'Euclide) Si A est euclidien, $(a,b) \in (A\setminus\{0\})^2$ alors l'algorithme d'Euclide permet de construire un PGCD d de a et b.

exemple ⑬ : si $d \in \mathbb{N}$ PGCD de $(m,n) \in (\mathbb{N}^*)^2$ alors $X^d - 1$ est un PGCD de $X^m - 1$ et $X^n - 1$

remarque ⑭ : l'algorithme d'Euclide permet également de construire $(u,v) \in A^2$ tel que $au + bv = d$

remarque ⑮ : l'existence du stathme sur A permet de rendre les preuves plus constructives

II - Applications des théorèmes importants dans un anneau principal

II - A. Théorème de Bézout, lemmes de Gauss et d'Euclide

déf (16) : On dit que $a, b \in A$ sont premiers entre eux si 1 est PGCD de a et b

théorème (17) : a et b premiers entre eux si et seulement si $\exists (u,v) \in A^2$, $au + bv = 1$

application (18) : si $(a,b,c) \in A^3$ et d PGCD de a et b alors l'équation diophantienne linéaire $ax + by = c$ admet une solution si et seulement si $d \mid c$

application (19) (lemme des noyaux) Si E K-espace vectoriel, $u \in End_K(E)$ et $(P_1, \dots, P_n) \in K[X]^n$ premiers entre eux deux à deux alors

$$\ker\left(\prod_{i=1}^{n} P_i(u)\right) = \bigoplus_{i=1}^{n} \ker(P_i(u))$$

corollaire (20) : Si $\chi_u = \prod_{i=1}^{n} P_i^{\alpha_i}$ avec les P_i distincts et irréductibles alors u est diagonalisable par blocs de taille $d_i = \dim(\ker(P_i^{\alpha_i}(u)))$

En particulier si χ_u scindé simple alors u est diagonalisable

proposition (21) (lemme de Gauss) Si a et b premiers entre eux et $a \mid bc$ alors $a \mid c$

exemple (22) : il faut que a et b soient premiers entre eux. En effet $4 \mid 6\times 2$ et $4 \nmid 6$, $4 \nmid 2$

proposition (23) (lemme d'Euclide) Si a et b sont premiers entre eux, $a \mid c$ et $b \mid c$ alors $ab \mid c$

corollaire (24) : Si a premier avec b et c alors a premier avec bc.

II - B. Théorème des restes chinois et système de congruence

déf (25) : Si I idéal principal de A alors A/I est l'ensemble quotient muni de l'addition et de la multiplication compatibles.

théorème (26) : (des restes chinois) Si $a_1, \dots, a_n \in A$ premiers entre eux alors $A/(\prod_{i=1}^{n} a_i) \simeq A/(a_1) \times \dots \times A/(a_n)$

exemple (27) : il faut que les a_i soient premiers entre eux deux à deux. En effet $\mathbb{Z}/6\mathbb{Z}$ (pas intègre) n'est pas isomorphe à $(\mathbb{Z}/2\mathbb{Z})^2$ (intègre)

application (28) : Si $(n_1, \dots, n_k) \in \mathbb{Z}^k$ premiers entre eux deux à deux et $(a_1, \dots, a_k) \in \mathbb{Z}^k$ alors il existe $x \in \mathbb{Z}$ (unique modulo $\prod_{i=1}^{k} n_i$) tel que $\forall i \in [\![1, k]\!]$, $x \equiv a_i [n_i]$

II - C. Théorème de décomposition en facteurs premiers

déf (29) : on dit que $p \in A$ est premier si $p \neq 0$, $p \notin A^\times$ et $\forall (b,c) \in A^2$, $p \mid bc \Rightarrow [p \mid b$ ou $p \mid c]$

déf (30) : on dit que $p \in A$ est irréductible si $p \neq 0$, $p \notin A^\times$ et $\forall (b,c) \in A^2$, $p = bc \Rightarrow [b \in A^\times$ ou $c \in A^\times]$

proposition (31) : p premier ssi (p) premier

lemme (32) : si p premier alors p irréductible

théorème (33) : p premier ssi p irréductible

remarque (34) : le caractère principal de A ne sert que dans le dernier des trois résultats précédents

théorème (35) : si $x \in A \setminus (\{0\} \cup A^\times)$ alors il existe $(p_1, \dots, p_k) \in \mathcal{P}^k$ (uniques à association et indexation près), $(v_{p_1}(x), \dots, v_{p_k}(x)) \in (\mathbb{N}^*)^k$ uniques et $\varepsilon \in A^\times$ unique tel que $x = \varepsilon \prod_{i=1}^{k} p_i^{v_{p_i}(x)}$

corollaire (36) : A est factoriel

application (37) : si $(a,b) \in (A \setminus (\{0\} \cup A^\times))^2$ alors :

* $d = \prod_{p \in \mathcal{P}} p^{\min(v_p(a), v_p(b))}$ est un PGCD de a et b
* $m = \prod_{p \in \mathcal{P}} p^{\max(v_p(a), v_p(b))}$ est un PPCM de a et b

III - Résolution de l'équation des deux carrés et anneau des entiers de Gauss $\mathbb{Z}[i]$

III-A. Equation des deux carrés

remarque (38) : on cherche à déterminer $(a,b) \in \mathbb{N}^2$ tel que $n = a^2 + b^2$ avec $n \in \mathbb{N}$.
(on note $\Sigma = \{n \in \mathbb{N}, \exists (a,b) \in \mathbb{N}^2, n = a^2 + b^2\}$)

exemple (39) : $0, 1, 2, 4, 5 \in \Sigma$ et $3, 6, 7 \notin \Sigma$

proposition (40) : si $n \equiv 3 [4]$ alors $n \notin \Sigma$

remarque (41) : si $n \in \Sigma$ alors $n = (a+ib)(a-ib)$

III. B - Anneau des entiers de Gauss $\mathbb{Z}[i]$

déf (42) : $N : \mathbb{Z}[i] \longrightarrow \mathbb{N}$, $z = a+ib \longmapsto z\bar{z} = a^2 + b^2$ est appelé norme

proposition (43) : $\mathbb{Z}[i]^\times = \{1, -1, i, -i\}$

proposition (44) : Σ est stable par multiplication

remarque (45) : on peut donc se ramener à $p \in \mathcal{P}$

proposition (46) : $\mathbb{Z}[i]$ est euclidien donc principal

III-C. Résolution de l'équation

lemme (47) : si $p \in \mathcal{P}$ alors $p \in \Sigma$ ssi p n'est pas irréductible dans $\mathbb{Z}[i]$

théorème (48) : si $p \in \mathcal{P}$ alors $p \in \Sigma$ ssi $p = 2$ ou $p \equiv 1 [4]$

théorème (49) : si $n \in \mathbb{N} \setminus \{0,1\}$ alors

$n \in \Sigma \iff \forall p \in \mathcal{P}, p \equiv 3 [4] \Rightarrow v_p(n) \in 2\mathbb{N}$